

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of

Digital Broadcast Content Protection

)
)
)
)

MB Docket No. 02-230

**COMMENTS OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.,
METRO-GOLDWYN-MAYER STUDIOS INC., PARAMOUNT PICTURES
CORPORATION, SONY PICTURES ENTERTAINMENT INC., TWENTIETH
CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS LLLP, AND
THE WALT DISNEY COMPANY**

Jon A. Baumgarten
Simon Block
Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street NW, Suite 800
Washington, DC 20036
(202) 416-6800

February 13, 2004

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
I. The Commission Should Adopt Market-Based Standards and Procedures for Authorizing New Output Protection Technologies and Recording Methods	2
II. The Scope of Prohibited Distribution Should Focus on the Local Environment.....	7
III. A Process Must Be Adopted To Determine If Technologies Have Been So Substantially Compromised That They Must Be Removed From Table A.....	8
IV. The Commission Should Require Cable Operators to Encrypt the Digital Basic Tier.....	11
V. The Broadcast Flag Will Not Unduly Interfere With the Construction of Software Demodulators	13
CONCLUSION.....	18

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Digital Broadcast Content Protection)	MB Docket No. 02-230
)	

**COMMENTS OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.,
METRO-GOLDWYN-MAYER STUDIOS INC., PARAMOUNT PICTURES
CORPORATION, SONY PICTURES ENTERTAINMENT INC., TWENTIETH
CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS LLLP, AND
THE WALT DISNEY COMPANY**

The Motion Picture Association of America, Inc. (“MPAA”), Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, and the Walt Disney Company hereby submits these Comments in response to the Commission’s Further Notice of Proposed Rulemaking.¹

INTRODUCTION

On November 4, 2003, the Commission adopted compliance and robustness rules requiring protection of Marked digital broadcast content in DTV demodulation devices and some peripheral transport-stream-processing products. Although the regulation cannot be in place for

¹ See Report and Order and Further Notice of Proposed Rulemaking, *Digital Broadcast Content Protection*, M.B. Docket No. 02-230, FCC 03-273 (rel. Nov. 4, 2003) (“Broadcast Flag Order”).

the 2004 manufacturing season,² the Commission's decision paves the way for a digital transition in which broadcast's role is assured.

I. The Commission Should Adopt Market-Based Standards and Procedures for Authorizing New Output Protection Technologies and Recording Methods

The Commission has requested comments in both the Broadcast Flag and the Plug & Play proceedings on “whether standards and procedures should be adopted for the approval of new content protection and recording technologies to be used with device outputs” on compliant products, and if so, what “types of content protection technologies that should be considered as a part of this process.” In substance, the answer to the standards questions in both proceedings should be the same. The same substantive considerations for ensuring the security and timeliness of new authorized outputs for Broadcast Flag-compliant devices apply in the Plug & Play context as well.³ Indeed, the list of Authorized Digital Output Protection Technologies and Authorized Recording Methods in the Broadcast Flag regulation (“Table A”) is designed to “piggy-back” on technologies approved by content owners for use in other venues. The entire basis of the proposal put forth in the Broadcast Flag proceeding and in the Broadcast Protection Discussion Group by the 5C companies, the MPAA, other content providers, and the Computer

² Some manufacturers have promised voluntary compliance with the Flag regulation by July 1, 2004. See Letter from David H. Arland, Director, Public & Trade Relations, Thomson Inc., to Marlene Dortch, Secretary, FCC (Oct. 8, 2003); Letter from Angela Lee, Manager, Government & Industry Relations, Mitsubishi Digital Electronics America, Inc. to Michael K. Powell, Chairman, FCC (Oct. 30, 2003); Letter from John I. Taylor, Corporate Vice President, Zenith Electronics Corp. to Michael K. Powell, Chairman, FCC (Oct. 30, 2003). The MPAA welcomes those promises and hopes and expects that other manufacturers will step forward now that the regulation has been adopted.

³ By proposing a unified set of standards for authorized technologies in both proceedings, we do *not* seek to import the numerical copy controls sometimes applicable to conditional access content into the broadcast television realm. Redistribution control, rather than numerical copy limitations, will remain the focus of the Broadcast Flag regulation. As we note in our comments to the Further Notice of Proposed Rulemaking in the Plug & Play proceeding, numerical copy control functionality and licensing terms will be required in authorized technologies for digital outputs and recordings of *non*-broadcast content from unidirectional cable products.

Industry Group (the “Joint Proposal”), is that output and recording technologies voluntarily approved for the protection of high-value DTV content distributed by cable and other channels are sufficient to protect broadcast DTV content.

Moreover, if the standards and procedures we propose in our separate Plug & Play comments are adopted for protection of non-broadcast content in Unidirectional Cable Products, we are prepared to support a regulation in this proceeding that would accord Table A authorization to any protection technology that is approved under the DFAST initial determination and review process.

Therefore, to the extent possible, a single set of criteria for authorizing content protection technologies should be adopted in both proceedings. As the 5C companies, the MPAA, and other content providers stated in comments filed earlier in the Broadcast Flag proceeding, the Commission should adopt standards and procedures that implement “a flexible, market-based approach under which a technology is authorized for Table A if it has been accepted in the relevant marketplace as a protection technology or it is just as effective as one that has.” Joint Initial Comments of the MPAA *et al.* at 22; *see also* Comments of the Digital Transmission Licensing Administrator LLC (“5C”) at 10. Under the Joint Proposal, any type of output technology, including technologies mapped to wireless signals and Digital Rights Management technologies, that prevents unauthorized redistribution, would be able to qualify for Table A. The MPAA welcomes and encourages manufacturers to come forward with new and innovative content protection technologies that meet the criteria put forward in the Joint Proposal and attached in revised form to these Comments as Appendix A.

As the MPAA has noted in the past, it is incredibly difficult to specify in advance all of the requirements that protection technologies must meet to provide a minimum level of

protection, while leaving the requirements general enough to accommodate different types of protection, both now and in the future. *See* Joint Reply Comments of the MPAA et al. at 18-19. While it is of course possible to state a vague “wish list” of possible features, such a list fails to give the Commission the concrete guidance necessary to allow it to decide in particular instances whether a given technology belongs on Table A or not. It was the near-impossibility of providing such specific guidance that led the MPAA and other industries in the BPDG to propose market-based criteria for Table A, supplemented by a simple benchmark test to be administered by the Commission. The Microsoft and HP proposal for “objective criteria,” cited in the Further Notice of Proposed Rulemaking, only serves to illustrate how difficult it is to devise a set of requirements that will both ensure that content is secure, yet does not “lock-in” protection technologies to a particular form of technology or to the particular standards we can envision today.

While the HP-Microsoft proposal refers to itself as providing “functional requirements,” it provides little guidance to the Commission or to manufacturers as to the threshold of protection that must be met. For example, the proposal states that “content protection methods should not create consumer confusion;” that “[a] content protection method should protect copyrighted information when it is transmitted among a variety of consumer devices;” that “[i]t should be relatively simple to implement the encryption algorithm;” that “[i]t must be possible to implement the authentication method;” that “[a]ny content protection method should be interoperable with other such methods;” that “[i]t should be technologically possible to upgrade the system in a relatively easy manner;” that “[i]t should be possible to revoke the ability of a device to receive protected content if the device is compromised;” and that “[t]he implementation of a content protection method should not compromise the performance of the

affected devices.” These subjective assertions do nothing to specify what technologies will qualify for Table A. For example, they do not answer the question of whether or not to authorize technologies which work only in connection with a particular device, are not interoperable with other Table A technologies, or are not relatively easy to upgrade.

However, the most glaring problem with the HP-Microsoft proposal is that it is incomplete. While the proposal addresses (in cursory fashion) the security that a Table A technology must provide to content as it is traveling over an output, nothing in the HP-Microsoft proposal – not a single paragraph – limits the reach of such outputs, or the extent of redistribution that a Table A technology qualifying under such criteria would permit. The HP-Microsoft proposal would allow onto Table A a technology that permits entirely indiscriminate redistribution. *That is, if encryption and authentication were added to a peer-to-peer file sharing utility, the HP-Microsoft proposal would allow it onto Table A.* Nothing about the proposal constrains Table A outputs, or outputs from Table A recordings, to a certain geographic location, or binds them to a certain person or persons, or limits their reach in any way. Obviously, such a proposal will not guarantee a level of protection for broadcast television equivalent to other, secure forms of distribution, which is the very point of the regulation.

The HP-Microsoft proposal thus does not sufficiently define the minimum levels of protection that must be afforded to content to qualify for Table A. The proposal states that the encryption method, for example, “should be difficult for consumers [to circumvent] using common means.” However, most consumers are not cryptographers. Without providing some sort of objectively measurable baseline, the HP-Microsoft proposal could be interpreted to allow ridiculously weak forms of encryption. The proposal provides no guidance as to how, and how

securely, devices must be authenticated. The proposal does not appear to rule out even a one-bit authentication message.

If Table A is allowed to be populated with weak protection technologies that do nothing to protect digital broadcast television, the entire purpose of the Broadcast Flag regulation – which is to prevent the migration of high-value content to more secure distribution channels – will be undermined. The Commission must ensure that Table A is populated not only with a wide variety of protection technologies, but a wide variety of secure protection technologies. The HP-Microsoft proposal, and others like it,⁴ fail to achieve that goal. Moreover, they will in all likelihood result in an authorization process that may become mired in procedural and substantive challenges, leading to a stagnant Table A with an insufficient population of technologies. No one desires and benefits from healthy competition among secure Table A technologies more than content providers.

We have added to Appendix A a provision that would prevent a technology from being authorized unless disclosure is made as to whether “use or triggering of the technology imposes any obligations upon a content owner’s or broadcaster’s use of an unencrypted over-the-air broadcast television signal,” and in the event of such obligations, the technology “may be turned off, bypassed, or otherwise not used and triggered at the content owner’s and broadcaster’s election and content owners and broadcasters are provided with facile means of such election.” *See* Appendix A § X.21(c)(9).⁵ This provision prevents a holder of patents in an authorized

⁴ *See also* Comments of Philips Electronics North America Corp. in Broadcast Flag at 15-18; Letter from Mike Godwin, Senior Technology Counsel, Public Knowledge to Marlene H. Dortch, Secretary, FCC (Oct. 29, 2003); Letter from Richard A. Beutel, Director, Government Relations, Dell, Inc., to Marlene H. Dortch, Secretary, FCC (Oct. 24, 2003).

⁵ It is anticipated that Section 76.1903 would either be amended consistent with this provision, or appropriate waivers would be issued if such a circumstance came to pass. We submit that, given the possibility of third-party intellectual property claims with respect to a Table A technology, the amended Section 76.1903 should also permit output control in the event that such claims surface after authorization of the technology.

digital output protection or secure recording technology from attempting to impose licensing obligations on content owners or broadcasters without their consent merely because content is transmitted over an output protected with that technology, or merely because encoding in the content invokes such technology.⁶ Without the opportunity to prohibit the use of such protected outputs in such circumstances, content owners and broadcasters may potentially be subjected to royalty claims and expensive litigation – possibly from multiple technology owners – that they could not avoid without forgoing protection of all of their content.

II. The Scope of Prohibited Distribution Should Focus on the Local Environment

The scope of prohibited distribution under our proposed criteria will essentially be self-defined by the marketplace criteria. In the case of applications made under such criteria, the Joint Proposal and our Appendix A require that they demonstrate how the output and recording controls “prevent unauthorized redistribution . . . (including redistribution over the Internet)”; and in the case of applications made under the “at least as effective as” criterion, the Joint Proposal and our Appendix A requires that such technologies be so effective “at protecting Unscreened Content and Marked Content against unauthorized redistribution (including unauthorized Internet redistribution).”

We believe that the focus of attention on unauthorized redistribution should be on whether a proposed technology affirmatively and reasonably constrains unauthorized distribution beyond the local environment; and that the language of the final regulations should be amended to make that clear. The “local environment” is the set of compliant, authorized devices within a

⁶ As of the date of this filing, the parties filing these Comments are not aware of any such patents or of any such patent claims being made. By raising this argument before the Commission, we of course are not conceding the validity of any future patent claim and are not waiving, and specifically reserve, any arguments that could be raised in the event of any future patent litigation.

tightly defined geographic area around a Covered Product. Mechanisms to define the local environment consist of: A) controls to limit distance from a Covered Product; B) limits on the scope of the network addressable by such Covered Products; and C) affinity-based controls used to approximate association of such set of devices with an individual or household. For example, the local environment of a Covered Product in a home consists of the set of authorized devices within or in the immediate vicinity (e.g., the yard, garage, or driveway) of that home but does not include Covered Products or devices located in a neighbor's home or operated by passers-by. Devices in an individual's car, RV, or boat are considered to be in the local environment of a Covered Product that is in an individual's home when the devices are in the immediate vicinity of that individual's home.

We do not believe that the notion of a "personal digital network environment" is appropriately addressed at this time. To begin with, that term has engendered considerable confusion. To the extent that the ambiguous notion of a "personal digital network environment" may go beyond localization, an attempt to regulate or define this area will inevitably risk substantial and continuing conflict with copyright law definitions of exclusive rights pertaining to performance and distribution, and significantly impair if not render impossible the efforts of copyright owners to protect those rights by technological means. It also will fundamentally impair and interfere with emerging business models designed to enhance consumer choice and consumer enjoyment of remote usage technologies.

III. A Process Must Be Adopted To Determine If Technologies Have Been So Substantially Compromised That They Must Be Removed From Table A

The Commission (as well as, *mea culpa*, certain earlier BPDG and related documents) uses the term "revocation" in asking several questions pertaining to a concept that we understand

as “delisting” or removal of technologies from Table A (herein “withdrawal”). We believe that in this context, “revocation,” “renewal,” and “withdrawal” connote different, albeit related, concepts.

“Revocation” in regard to content protection technologies generally means the disabling of limited numbers of compromised devices and unlawful clones because particular identifications associated with those devices have been lost or stolen. “Renewal” and “renewability” generally refer to more substantial corrections of more widespread compromise of deployed devices (e.g., by downloading fundamental adjustments to the operation of the protection technology). (Neither revocation or renewability generally impair the operation of unrelated functionalities in the same device.) The capacity and mechanisms for both revocation and renewability are integral features of content protection technologies themselves. We would expect technologies that attain Table A under our proposed (or, indeed any other) criteria will include these features.⁷

Nevertheless, no matter how rigorous the Table A authorization process is and notwithstanding the technical capacity of authorized technologies, there will always be some chance that a protection technology is substantially compromised. A substantial compromise of a Table A technology would have serious and far-ranging deleterious consequences; for example, the flooding into the marketplace of subsequent new devices containing such substantially compromised technologies. New devices would continue to be made and sold that will make unauthorized, indiscriminate redistribution of broadcasts simple, inexpensive, and devastating. Indeed, there is little doubt that in some quarters, the compromised technologies will become marketed *features* of new devices, rather than seen as the threats to content owners

⁷ We will consider the implementation of revocation and renewability features as important factors in reviewing proposed technologies under the Commission's Interim Process for Table A.

and the vitality of the free broadcasting system that they are. This result must be avoided if at all possible. A Table A technology is likely to be used not only for broadcast and cable television content, but also for most other forms of high-value content as well. Thus, a substantial compromise would imperil many different distribution channels simultaneously. Given this risk, the Broadcast Flag regulation must include some provision in the event that this worst case comes to pass. That provision is the *withdrawal* of Table A authorization, under carefully considered circumstances.⁸

The process proposed in the criteria attached here allows the Commission to consider every possible means of mitigating the effect of a substantial compromise. Under the standard contained in the Joint Proposal, content owners would first be required to demonstrate that the Table A technology in question has been “substantially compromised in relation to its ability to protect Unscreened Content and Marked Content from unauthorized redistribution (including unauthorized Internet redistribution).” *See* Appendix A § X.23(b)(2). That showing would have to include a description of the steps that could be taken to ameliorate the effect of delisting on consumers and manufacturers. In response, the technology manufacturer would then have an opportunity to demonstrate the efforts that have been taken to repair the technology. Both parties would also be required to address several other factors in their submissions: the protection of Unscreened Content and Marked Content from unauthorized redistribution (including from unauthorized Internet redistribution), and the impact on interested parties for each scenario. If, after carefully weighing this evidence, the Commission finds that the compromise of the technology is substantial, the Commission would need to rescind its authorization as a Table A

⁸ “Withdrawal” of Table A authorization is also different from the disqualification of a listed technology as a benchmark for “at least as effective” criterion for Table A. *See* Section X.23(a) of Appendix A. A disqualified technology is not removed from Table A and may continue to be employed in covered Products.

technology. In such a case, the only alternative would be the insecurity of the entire system, undermining the very purpose of the Broadcast Flag regulation.

IV. The Commission Should Require Cable Operators to Encrypt the Digital Basic Tier

The Commission has requested comment on whether “cable operators that retransmit DTV broadcasts may encrypt the digital basic tier in order to convey the presence of the ATSC flag through their conditional access system.” We believe that, on a going-forward basis, cable operators should be *required* to encrypt the digital basic tier.

Section 76.630 of the Commission’s rules prohibits “scrambl[ing] or encrypt[ing] signals carried on the basic service tier.” The Commission has never clarified whether this provision is intended to cover all basic service tiers, including digital basic, or whether it applies only to analog. *See* Report & Order, *Compatibility Between Cable Systems and Consumer Electronics Equipment*, P.P. Docket No. 00-67 ¶ 32 (rel. Sept. 15, 2000). The Commission should take the opportunity of the Broadcast Flag FNPRM to clarify once and for all that Section 76.630 does not apply to the digital basic tier, and that in order to protect retransmitted digital broadcast content, cable operators must in the future encrypt the digital basic tier.

For one thing, encryption of the digital basic tier would permit cable operators to, when the time comes, add 1024-QAM modulation schemes to their systems without the need for another rulemaking. Currently, those retransmitting of digital broadcast content have two options under the rules: they can encrypt the retransmitted content, using whatever modulation scheme they prefer, or they may retransmit in the clear, so long as they use 8-VSB, 16-VSB, 64-QAM, or 256-QAM. Thus, in order to add 1024-QAM modulation, a cable operator will either have to be allowed to encrypt the 1024-QAM signal, or the operator will have to petition the

FCC to add 1024-QAM as a covered modulation scheme. Encryption of the digital basic tier by cable operators, as is already done by satellite operators with no ill effects, will avoid the need for another rulemaking every time cable operators wish to add a new modulation scheme.

Second, cable operators should be able to protect copyrighted content, including content made available on the digital basic tier and through retransmitted broadcasts, from unauthorized reception. *See* NCTA Reply Comments at 4 (filed Feb. 20, 2003). Requiring encryption of the digital basic tier will address the potential security problem caused by digital content being transmitted within the receiving box in the clear. In any event, the Commission should require encryption where it can be accomplished without creating legacy issues; all else being equal, encrypted content is much better protected than unencrypted content.

Third, requiring such encryption may also make cable services more compatible with certain home networking technologies. For example, an encrypted signal can more efficiently trigger 5C protection in a licensed device. In addition, an encrypted, unprocessed signal may be passed to various devices in the home from the receiving device via a Robust Method transfer before the signal is processed. However, this should not be interpreted to mean that Robust Method transfers should be allowed for processed, Marked Content as well.⁹

As the MPAA has previously stated, Section 73.9003(a)(4) was devised for the narrow purpose of accommodating products that only demodulate, but do not engage in Transport Stream Processing, and output an uncompressed, unprocessed signal to a separate product for processing, what is now called a Peripheral TSP Product. Such an uncompressed, unprocessed

⁹ *See* NCTA Reply Comments at 5-7; Petition for Reconsideration of the NCTA at 6-10. For reasons that will be explained in more detail in our forthcoming opposition to NCTA's Petition for Reconsideration, permitting the use of Robust Methods generally as a home networking technology would largely eliminate the need for Table A and undermine the entire regulation. The use of Robust Method outputs must therefore be combined to the single, narrow exception that was agreed to in the Broadcast Protection Discussion Group. *See* Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group ¶ 5.4 (June 3, 2002).

signal is at less risk of interception and redistribution than content that has undergone Transport Stream Processing. Since the upstream product in such a case does not process the signal, it cannot check for the Flag; there is thus no set of circumstances in which such an upstream device would be outputting anything other than Unscreened Content. There was therefore no reason to create a similar exception for outputs of Marked Content, which would have simply created a vast and unnecessary loophole. Furthermore, home networking is feasible without Robust Method outputs for Marked Content; indeed, the very point of a Table A digital output protection technology is to allow secure home networking from a compliant demodulator. The exception proposed by NCTA would obviate the need for a Table A at all. The Commission should decline to eliminate Table A and should reject NCTA's proposed inclusion of Robust Method outputs for Marked Content.

While the Commission, strictly speaking, only requested comment on whether cable operators should be allowed to "encrypt the digital basic tier in order to convey the presence of the ATSC flag through their conditional access system," the same considerations mentioned above apply equally well to the rest of the digital basic tier. High-value content is made available over cable channels as well, and it would be incongruous to protect digital broadcast television from migration to more secure distribution channels, but fail to protect cable from the same threat. The Commission should therefore require that the entire digital basic tier be encrypted by cable operators.

V. The Broadcast Flag Will Not Unduly Interfere With the Construction of Software Demodulators

The Commission has also requested comment on "the interplay between a flag redistribution control system and the development of open source software applications,

including software demodulators, for digital broadcast television.” The Broadcast Flag regulation applies equally to software and hardware demodulators, and there is no justification for any distinction. The regulation adopted by the Commission requires manufacturers of covered demodulators to sell or distribute such demodulators in compliance with the regulation. A “Demodulator” is “a component, or set of components, that is designed to perform the function of 8-VSB, 16-VSB, 64-QAM or 256-QAM demodulation and thereby produce a data stream for the purpose of digital television reception.” 47 C.F.R. § 73.9000(g). Any exception to this definition for demodulators with software components would open a huge loophole and severely diminish the effectiveness of the protection scheme established by the regulation. Thus, demodulators with software components, including open source demodulation functions, must comply with the Compliance and Robustness Rules adopted in Subpart M of Part 73.

If open source programmers wish to design a software component of an 8-VSB, 16-VSB, 64-QAM, and 256-QAM demodulator, they have three options: they can choose not to sell or distribute their demodulator in interstate commerce; they can either incorporate their software components into a compliant Demodulation Product, which is robust against attack and has only the outputs and integrated recording methods permitted under the regulation; or they can sell or distribute their software demodulation component to a Bona Fide Reseller for incorporation into a compliant product. There is no evidence that the need to comply with the Broadcast Flag regulation would pose any significant burden on designers of open source software demodulation components. There is no incompatibility between open source and security. Even Linus Torvalds, the founder of the open-source Linux operating system, has asserted that open-source software is fully compatible with secure DRM technology.¹⁰

¹⁰ See John Borland, *Linux Founder Opens Door to DRM*, CNET News.com (Apr. 24, 2003), available at <http://news.com.com/2100-1016-998292.html>.

There is an increasing need in the marketplace for secure equipment and software programs. For example, many consumers are protecting their home computers against intrusions by erecting firewall barriers and establishing encryption on their wireless networks. The Broadcast Flag regulation is simply part of this trend toward tamper-resistant devices. Open-source software programmers have already begun developing secure applications, and will continue to do so in the future. The Broadcast Flag regulation thus represents merely an expansion of these efforts that will help create an entirely new market in protection technologies. We expect open-source software will play an important role in the competition for secure software that is robust against tampering and compliant with the Broadcast Flag regulation.

In any event, open-source software demodulation products already have to comply with a number of the Commission's rules, with no apparent ill effects. For example, open-source demodulation products, like all unintentional radiators, must comply with the Commission's interference rules. *See* 47 C.F.R. §§ 15.5, 15.15(a), 15.109. Those rules place certain requirements on how devices are constructed, with, in the case of television sets, verification by the manufacturer submitted to the Commission. *See id.* § 15.101. The open-source software demodulation product must include a closed-captioning decoder compliant with Section 15.122. If offered for sale or resale to the public, the open source demodulation product must adequately receive all channels. *See id.* § 15.117(b). If used with a screen thirteen inches or wider, the open-source demodulation product must include channel-blocking capability. *See id.* § 15.120. If a software-based demodulator is capable of automatically scanning frequencies other than those used for radio, television, or NOAA weather broadcasts, then it must be "incapable of operating (tuning), or readily being altered by the user to operate," within the bands assigned to cell phones. *Id.* § 15.121(a)(1). The device must also be "designed so that the tuning, control

and filtering circuitry is inaccessible.” *Id.* § 15.121(a)(2). If the device contains a transmitter, such that it is a “Software Defined Radio,” then the software component must be secure against tampering, *see id.* § 2.932(e), and all changes to the software must be approved by the Commission prior being marketed, *see id.* § 2.1043(b)(3). The Broadcast Flag regulation does not represent a material departure from previous device regulations with respect to its impact on open-source programmers of software demodulators.

The Electronic Frontier Foundation (“EFF”) has expressed a concern that the Broadcast Flag regulation would prohibit publication of the source code of the software components of a demodulation product capable of receiving and demodulating ATSC broadcasts. *See* Letter from Fred von Lohmann to Chairman Powell at 2 (Oct. 28, 2003). The EFF claims that the regulation of software in such a manner would be a violation of the First Amendment. Accordingly, the EFF requests that an exception be drawn for Covered Demodulators containing software components.¹¹

The EFF’s arguments fail for three reasons. First, the EFF’s request for an exception for demodulators is based on the erroneous assumption that no “threat of widespread unauthorized Internet redistribution of free, over-the-air ATSC broadcast content” exists, and that therefore no regulation of software demodulators is necessary. *See id.* at 3. The Commission, however, has already found that such a threat “is forthcoming and preemptive action is needed to forestall any potential harm to the viability of over-the-air television.” Broadcast Flag Order 4. Given the

¹¹ Although the EFF states that SDRs “where software . . . perform[s] all the modulation and demodulation necessary to send and receive radio signals . . . already exist,” in fact the Software Defined Radio promoted on the GNU Radio website requires several hardware components, including an A/D converter and a cable modem tuner module. *See* GnuRadio: HowtoHdTv, <http://comsec.com/wiki/HowtoHdTv>. Thus, more accurately, the EFF is requesting an exception for any demodulator that includes a software component.

reality of the threat, the regulation of VSB and QAM demodulators is necessary, whether they have software components or not.

Second, the EFF's First Amendment claim is based on the flawed premise that any regulation of software impermissibly impinges on speech. However, courts have already considered and rejected this argument. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 451 (2d Cir. 2001) ("[The] realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, i.e., functional and expressive elements."). In fact, the Broadcast Flag regulation no more impinges on speech in regulating software demodulators than in regulating hardware demodulators, which after all may have some expressive component that other hardware engineers may appreciate. Such expressive components have never been held to prevent the Commission from regulating broadcast television and radio receivers, nor should such expressive components be held to exempt software demodulators from Commission regulation. Notably, the EFF's argument would apply just as well to the regulation of scanning receivers with software components or to Software-Defined Radios. Such a laissez-faire attitude toward software products would be extremely unwise as more and more functions become capable of being performed in software.

Third, neither the EFF nor any other party has demonstrated how, if at all, the Flag regulation would prohibit the publication of open-source demodulator software. While there has been much speculation on this issue, no one has identified a rule that would require such a result. There is no rule that prohibits schematics of Covered Products from being released, for example, or software source code from being published. The Robustness Rules adopted by the Commission (as well as those in the Joint Proposal) do not require that the code of a software component of a Covered Product not be visible to the end user; they require only that the

Covered Product, including compiled source code and hardware components, not be constructed such that the Compliance Rules provided in the Broadcast Flag regulation can be circumvented. In other words, the Robustness Rules require only that if the object code of a compliant Covered Product is altered, that it either (1) continue to be compliant, or (2) cease functioning.

The regulation also requires that software components that are capable of performing the specified forms of demodulation must be sold or distributed in compliant form or to Bona Fide Resellers that will put the demodulator in a compliant product. Open source programmers thus have at least two options in collaborating on source code: they may share the code among themselves in segments that do not rise to the level of a component or one of a set of components that performs 8-VSB, 16-VSB, 64-QAM, or 256-QAM modulation; or they may transfer the code only to Bona Fide Resellers. No party has introduced any reason to believe that open source programmers cannot meet these requirements. Accordingly, the vague assertions of harm from parties already inalterably opposed to the Broadcast Flag and content protection in general should not prompt the Commission to make any exceptions to the Broadcast Flag regulation.

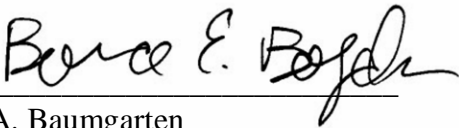
CONCLUSION

The Commission has undertaken a huge burden in shepherding the digital transition with respect to both broadcast television and conditional access content. The Commission has met that challenge by adopting the Broadcast Flag regulation and by considering in this rulemaking the procedures for approving content protection technologies for DTV receivers taking advantage of those already approved for use with cable Plug & Play devices. Adoption of the proposed regulations attached here will help complete this journey successfully and ensure that

broadcast television is preserved and that high-quality content is made available to consumers in new and exciting ways.

Respectfully submitted,

THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.
METRO-GOLDWYN-MAYER STUDIOS INC.
PARAMOUNT PICTURES CORPORATION
SONY PICTURES ENTERTAINMENT INC.
TWENTIETH CENTURY FOX FILM CORPORATION
UNIVERSAL CITY STUDIOS LLLP
THE WALT DISNEY COMPANY

By: 

Jon A. Baumgarten

Simon Block

Bruce E. Boyden

Proskauer Rose LLP

1233 Twentieth Street NW, Suite 800

Washington, DC 20036

(202) 416-6800

Counsel for the Commenting Parties